

To Fix the Technology Glitches, SEC Imposes New Regulation SCI on the Markets

Detailed rules will become effective February 2015, with compliance required by November 2015.

On November 19, 2014, the Securities and Exchange Commission (the Commission) adopted new rules for technology infrastructure in the US securities markets. These rules combine to form Regulation Systems Compliance and Integrity (Regulation SCI). Regulation SCI imposes requirements on key market participants in order to strengthen the markets' technology infrastructure, reduce the occurrence of systems issues and improve the resiliency for when systems problems do occur.

Executive Summary

Regulation SCI applies to self-regulatory organizations, certain alternative trading systems (ATSs) that exceed volume thresholds, plan processors, and certain exempt clearing agencies which are currently subject to the Commissions Automation Review Policy (ARP) (collectively referred to as SCI entities). Alternatively, Regulation SCI does not cover securities futures exchanges, the NFA, or ATSs that exclusively trade municipal or corporate debt. While the Commission noted that it would take a "measured approach" towards incremental expansion and it kept the definition of SCI entity fairly narrow, the Commission also acknowledged "other categories of entities not included within the current definition of SCI entity that, given their increasing size and importance, could pose risks to the market should an SCI event occur." Specifically, in the adopting release the Commission listed some future candidates — non-ATS broker-dealers, security based swap dealers, investment advisers, investment companies and transfer agents — for the expanded scope. In fact, Commission Chair Mary Jo White has directed the Commission Staff to evaluate the prospect of implementing an "SCI-like framework to cover such key market participants."¹

For SCI entities, Regulation SCI imposes obligations for the entities, their personnel and their technology systems. SCI entities must implement and enforce policies and procedures related to capacity, integrity, resiliency, availability and security of its SCI systems. These requirements cover software development, stress tests, collection of market data, system monitoring, cybersecurity, business continuity and disaster recovery planning, periodic reviews and plans to promptly remedy any deficiencies. Finally, SCI entities must establish procedures to identify and periodically review who they have designated as "SCI personnel" responsible for SCI systems. Regulation SCI does not provide a safe harbor for SCI entities; instead, it lays out minimum requirements for the policies and procedures. In contrast, there is a safe harbor available for individuals.

In the event certain “SCI events” occur, Regulation SCI imposes a variety of reporting obligations at the time of the event, as the entity seeks to correct the problem, and after the issue is resolved. The nature and severity of the event will determine how widely these reports are disseminated.

Regulation SCI also requires periodic testing of SCI systems, reporting on the results of those tests and reporting on any material changes made to such systems. This process must include senior management review. Similarly, Regulation SCI requires industry or sector-wide business continuity/disaster recovery testing.

Lastly, Regulation SCI imposes recordkeeping requirements, which also include providing the Commission with access to such records upon request.

A note on the use of third parties: All SCI entities are responsible for the conduct of third parties operating SCI systems, critical SCI systems and indirect SCI systems on their behalf. Accordingly, the Commission may demand access to the pertinent files, intellectual property, etc. of such third parties and has suggested that SCI entities reevaluate their relationships with vendors that cannot or will not conform — as such non-conformance will be imputed to the SCI entity itself.

Detailed Rule Summary

Rule 1000 – Scope and Definitions

Rule 1000 of Regulation SCI sets forth the scope and definitions of the regulatory scheme. Significant definitions include: SCI entity, SCI systems and SCI events — detailed below.

SCI entity

SCI entities include SCI self-regulatory organizations (SCI SRO), SCI alternative trading systems (SCI ATS), plan processors and exempt clearing agencies subject to the Automation Review Policy (ARP).

- *SCI SRO.* The definition of SCI SRO generally tracks the definition of an SRO as set forth in § 3(a)(26) of the Securities Exchange Act of 1934 (Exchange Act), and includes national securities exchanges registered under § 6(b) of the Exchange Act, registered securities associations, registered clearing agencies and the Municipal Securities Rulemaking Board (MSRB). However, Regulation SCI excludes exchanges that list or trade securities futures products that are notice-registered with the Commission under § 6(g) of the Exchange Act, as well as limited national securities associations registered pursuant to § 15A(k) (e.g., securities futures exchanges and the National Futures Association).
- *SCI ATS.* The definition of SCI ATS is based on volume thresholds. An ATS is an SCI ATS if, during at least four of the last six months, it had either:
 - (a) with respect to NMS stocks either (i) 5% or more in any single NMS stock, and 0.25% or more in all NMS stocks, of the average daily dollar volume reported by an effective transaction reporting plan, or (ii) 1% or more, in all NMS stocks, of the average daily dollar volume reported
 - (b) with respect to non-NMS equity stocks that are reported to an SRO, 5% or more the average daily volume as calculated by the SRO to which such transactions are reported.

ATSS that trade only municipal securities or corporate debt are excluded from the definition of SCI ATS.² A dark pool may be considered an SCI ATS if, as an ATS, it meets the volume thresholds stated above.

- *Plan Processor.* The definition of plan processor tracks Rule 60(b)(55) of Regulation NMS. Under Regulation SCI, a plan processor is any SRO or securities information processor acting as an exclusive processor in connection with the development, implementation and/or operation of any facility contemplated under an effective national market system plan.
- *Exempt Clearing Agency.* The definition of exempt clearing agencies covers exempt clearing agencies subject to ARP. An exempt clearing agency is an entity that has received an exemption from registration with the Commission as a clearing agency under § 17A of the Exchange Act, and whose exemption contains conditions that relate to the Commission's ARP, or any regulation that supersedes or replaces such policies.

Regulation SCI is intended to cover the historical reach of the ARP Inspection Program and existing Rule 301 of Regulation ATS, while also including additional entities that the Commission believes play a significant role in US securities markets. The Commission may expand the scope of Regulation SCI in the future to cover additional market participants such as non-ATS broker-dealers, security-based swap dealers, investment advisers, investment companies, transfer agents and other key market participants.

SCI systems

Regulation SCI classifies three distinct types of systems: SCI systems, critical SCI systems and indirect SCI systems.

- *SCI System.* An SCI system is any computer, electronic, technical, automated or similar system, with respect to securities, that directly supports any of the following: (i) trading, (ii) clearance and settlement, (iii) order routing, (iv) market data, (v) market regulation or (vi) market surveillance. This classification extends to all systems, whether private, public or operated by a third-party on behalf of an SCI entity. However, Regulation SCI is limited to production systems that relate to securities; it does not include systems used for development of testing or those systems used for non-market data such as filings or public disclosures (see e.g., Rule 1001(a)).
- *Critical SCI System.* A critical SCI system is a subset of a general SCI system. A critical SCI system is an SCI system that either: (a) directly supports one of six essential functions the Commission believes crucial to market functionality, or (b) provides a crucially important functionality to the securities markets for which there is no adequate alternative. The six essential functions are: (i) clearance and settlement; (ii) openings, re-openings and closings on primary markets; (iii) trading halts; (iv) IPOs; (v) consolidation of market data; and (vi) exclusively listed securities. As is the case with all other SCI systems, critical SCI systems operated by third parties on behalf of the SCI entity will be subject to regulation.
 - Critical SCI systems are subject to stricter requirements than other SCI systems because they pose a higher risk to the securities markets. While all SCI systems must provide assurance of adequate capacity, integrity, resiliency, availability, security, recovery and disclosure, these requirements are heightened for critical SCI systems.
- *Indirect SCI System.* An indirect SCI system is any system that, if breached, would be reasonably likely to pose a security threat to an SCI system. Indirect SCI systems are not as heavily regulated as SCI systems. SCI entities must self-assess and determine which of their systems meets this

definition. The key to this assessment is whether the system is effectively physically or logically separated off from all SCI systems. In order to create an effective separation, an SCI entity must establish and adopt a scheme of reasonably designed and effective controls to insulate its SCI systems.

- While indirect SCI systems are still subject to some regulations imposed on SCI systems, many requirements differ. For example, like SCI systems, indirect SCI system regulations attach to SCI entities whether those entities maintain their own indirect SCI systems or rely on a third party. However, unlike SCI systems, indirect SCI systems are not subject to regulation under all the provisions of Regulation SCI. Rather, indirect SCI systems are only subject to the rules regarding policies and procedures that ensure operational capability (see Rule 1001(a)), SCI events (see Rule 1002), material changes in the system (see Rule 1003(a)) and record-keeping and electronic filing (see Rules 1005-1007).

All SCI entities are responsible for the conduct of third parties operating SCI systems, critical SCI systems and indirect SCI systems on their behalf. Accordingly, the Commission may demand access to the pertinent files, intellectual property, etc. of such third parties and has suggested that SCI entities reevaluate their relationships with vendors that cannot or will not conform, as such non-conformance will be imputed to the SCI entity itself.

SCI event

Certain obligations of an SCI entity under Regulation SCI are only triggered by an "SCI event." The three categories of SCI events are: (1) systems disruptions, (2) systems compliance issues and (3) systems intrusions. There is no materiality threshold on any category of SCI event, which means that even de minimus events are defined as SCI events and may trigger additional requirements for an SCI entity.

- *Systems Disruption. A systems disruption is an event that disrupts or significantly degrades the normal operation of an SCI system. An SCI entity has discretion in determining whether an issue should be categorized as a disruption. Some examples of a systems disruption include: a failure to maintain service level agreements or constraints, a switchover to backup equipment without likelihood of near-term recovery, the loss of use of a system, the loss of data, significant delays in processing or ability to disseminate market data and an unusual queuing of data or messages. Furthermore, regularly scheduled outages or maintenance can be classified as normal operations and thus not an SCI event.*
- *Systems Compliance Issue. A systems compliance issue is an event that causes an SCI system to operate in a manner that does not comply with the Exchange Act or the entity's own rules and governing documents.*
- *Systems Intrusion. A systems intrusion is any unauthorized entry into an SCI systems. This type of event include all types of unauthorized entry, regardless of the identity of the person or the nature of the entry. An intrusion does not include unsuccessful attempts at unauthorized entry. Some examples of an intrusion include: the introduction of malware, unauthorized access by employees due to system weakness (whether intentional or inadvertent) and intrusions into indirect SCI systems.*

Rule 1001 – Written Policies and Procedures

Rule 1001 lays out the obligations of SCI entities to implement written policies and procedures related to (i) capacity, integrity, resiliency, availability and security of its SCI systems, (ii) systems compliance with the Exchange Act and (iii) identifying responsible SCI personnel.

Capacity and Security Policies. Each SCI entity must maintain and enforce written policies and procedures reasonably designed to ensure that its SCI systems — and for purposes of security standards — indirect SCI systems, have levels of capacity, integrity, resiliency, availability and security adequate to maintain the SCI entity's operational capacity and promote the maintenance of fair and orderly markets. At a minimum, such policies and procedures must address:

- *The establishment of reasonable current and future technological infrastructure capacity planning estimates;*
- *Periodic capacity stress tests;*
- *Programs to review and update systems development and testing methodology;*
- *Regular reviews and testing of systems, including backup systems, to identify vulnerabilities pertaining to internal and external threats, physical hazards and natural or manmade disasters;*
- *Business continuity and disaster recovery (BC/DR) plans that include maintaining backup and recovery capabilities with sufficient resiliency and geographical diversity, and that are reasonably designed to achieve next-day business resumption of trading and two-hour resumption of critical SCI systems following a wide-scale disruption;³*
 - *Recovery Timeframe.* The recovery times included in Regulation SCI are goals and not inflexible deadlines. Nonetheless, neither requirement is dependent upon the time of day that the loss of functionality occurred, even if the time of day of a disruption can effect actual recovery times. SCI entities — especially clearing agencies — should endeavor to take all steps necessary to effectuate end-of-day settlement.
 - *Geographic diversity.* While there is no minimum distance, backup sites should not rely on the same infrastructure components, such as for transportation, telecommunications, water supply and electric power.
- *Standards for the design, development, testing, maintenance, operation and surveillance of systems in a manner that facilitates the successful collection, processing and dissemination of market data;*
 - *Market Data.* Market data here includes not only consolidated market data, but also proprietary market data. As such, SCI systems supporting such market data are subject to Regulation SCI requirements.
- *The monitoring of SCI systems, and for purposes of security standards, indirect SCI systems, to identify potential SCI events;*
- *Periodic review of the effectiveness of these policies and procedures, as well as prompt action to remedy any deficiencies.*

Regulation SCI gives the SCI entities the flexibility to determine when and how to conduct stress tests and reviews. “Reasonably designed” means consistent with current SCI industry standards which relates to IT practices that are widely available to IT professionals in the financial sector and issued by an authoritative body.⁴ Concurrent with Regulation SCI, the Commission Staff issued guidance to SCI entities on developing policies and procedures consistent with “current SCI industry standards.”⁵ However, compliance with these standards is not the exclusive means of compliance.

Exchange Act Compliance Policies. Each SCI entity must establish, maintain and enforce written policies and procedures reasonably designed to ensure that its SCI systems operate in a manner that complies with the Exchange Act and their governing documents.

Regulation SCI sets forth minimum requirements for systems compliance policies and procedures at the entity level. Under Rule 1001(b), the written policies and procedures for Exchange Act compliance must provide for:

- *Testing of all SCI systems and any changes prior to implementation;*
- *A system of internal controls;*
- *A plan for assessments of SCI systems designed to detect systems compliance issues (a combination of ongoing monitoring and assessments);*
- *A plan for coordination and communication between regulatory and other personnel of the SCI entity regarding SCI systems; and*
- *Periodic review of effectiveness of such policies and procedures, and prompt action to remedy any identified deficiencies.*

While Regulation SCI imposes obligations on SCI entities, as with all other Exchange Act and rule violations, there is potential for secondary liability for an individual who aided and abetted or caused a violation. Thus, Regulation SCI does include a safe harbor for individuals. This safe harbor sets forth conditions that an individual seeking to avoid secondary liability for violations by an SCI entity must meet. The burden of proof is on the person seeking the safe harbor. Under the safe harbor, personnel of an SCI entity shall be deemed not to have aided, abetted, counseled, commanded, caused, induced or procured the violation by an SCI entity of Rule 1001(b) if the person (i) reasonably discharged the duties and obligations under the SCI entity’s policies and procedures; and (ii) had no reasonable cause to believe the policies and procedures relating to the system for which they were responsible, or had supervisory responsibility, were not established, maintained or enforced in accordance with Rule 1001(b) in any material respect.

Responsible SCI Personnel. Rule 1001(c) sets forth the requirements for an SCI entity to establish, maintain and enforce written policies and procedures that include (i) criteria to identify “responsible SCI personnel” (see Rule 1002 below) and (ii) escalation procedures to quickly inform SCI personnel of potential SCI events. SCI entities must periodically review the effectiveness of such policies and procedures and take prompt remedial action should they identify any deficiencies.

Rule 1002 – Obligations Related to SCI Events⁶

Rule 1002 addresses the reporting obligations when responsible SCI personnel have a reasonable basis to conclude that an SCI event has occurred. Once responsible SCI personnel have determined that an

SCI event has occurred, an SCI entity has three obligations: (i) take corrective action, (ii) notify the Commission and in some cases, (iii) disseminate information regarding an SCI event.

Trigger. The obligations under Rule 1002 are all triggered when “responsible SCI personnel” have a “reasonable basis” to conclude that an SCI event has occurred. “Responsible SCI personnel” are senior personnel that have responsibility for a particular system. SCI entities have discretion in determining which personnel to designate and also have the flexibility to delegate some responsibilities to personnel other than senior management. Regulation SCI imposes obligations only on entities and does not apply directly to personnel. The standard of Rule 1002 that personnel have a “reasonable basis” to conclude that an SCI event has occurred allows an SCI entity flexibility in determining if the obligations of Rule 1002 should apply. When determining whether an SCI event has occurred, responsible personnel should gather relevant information and perform an initial analysis and assessment.

Corrective Action. Taking corrective action requires an SCI entity to respond with appropriate steps necessary to remedy the problem causing the SCI event and mitigate its effects. An SCI entity has discretion in determining the appropriate corrective action but should do so as soon as reasonably practicable. An appropriate response may include: determining the scope of the event and its cause, determining the event’s impact, following internal procedures and regaining full functionality of a system.

Notification. Notification of the Commission requires an SCI entity to first determine whether an SCI event is de minimus or not. A de minimus event has minimal or no effect on operations. For de minimus events, an SCI entity must only maintain records of the event internally and submit a quarterly report to the Commission summarizing all de minimus SCI events during the quarter.

Notification of the Commission for SCI events that are not de minimus is a four step process. Reporting obligations are completed when an SCI entity submits a final report.⁷

- *First, once a determination has been made that an SCI event has occurred, an SCI entity must immediately notify the Commission of the SCI event by phone or in writing (email or Form SCI), even if the communication is outside of normal business hours.*
- *Second, an SCI entity must submit written notification to the Commission within 24 hours of determining that an SCI event has occurred. The notification need not be a complete or wholly accurate assessment, but must be made on a good faith basis. The notification should include: a description of the SCI event, an assessment of the potential effect on the market and market participants, the steps taken by the SCI entity to resolve the issue, when the SCI event was resolved or will be resolved and any other pertinent information.*
- *Third, after the initial written notification, an SCI entity must provide updates to the Commission to correct any materially incorrect information or provide new material information. Updates must be provided on a regular basis until the event is resolved (or as requested by the Commission) and can be provided either orally or in written form. An event is resolved when the event no longer meets the definition of an SCI event (see Rule 1000).*
- *Fourth, an SCI entity must submit a final written notification to the Commission once an SCI event is resolved and the SCI entity’s investigation is closed. The final report must contain a detailed description⁸ of the entity’s assessment and response to the SCI event, a copy of any information disseminated pursuant to Rule 1002(c)⁹ and an analysis of any loss to parties. If the event and investigation is resolved within 30 days of its occurrence, the final report must be filed within 5 days after resolution; however, if the event is not resolved within 30 days, an SCI entity must submit an*

interim report within 30 days of the event with the same information as a final report to the extent known at the time and also submit a final report within 5 days of resolution.

Dissemination. The dissemination requirements of Rule 1002(c) vary depending on the nature of the SCI event.

- For SCI events that relate only to market regulation or surveillance systems¹⁰ or events that are deemed to have a de minimus impact, no information dissemination is required.
- For SCI events that are either systems disruption or systems compliance issues, an SCI entity must promptly share information about the system affected and a summary of the event; further dissemination, including a detailed description, a current assessment of the effect of the event, the expected resolution and any updates, must be shared when known by the entity.
- For SCI events that are systems intrusions, an SCI entity must promptly share a summary description of the intrusion. The summary description should include a description of the corrective action taken and when the intrusion is expected to be resolved. However, an SCI entity may delay disseminating information about a systems intrusion if sharing the information would compromise the security of its systems or the investigation of the intrusion.

The recipients of the required dissemination for an SCI event vary depending on whether the event is a major SCI event or not. For major SCI events,¹¹ the required information must be disseminated to all of the SCI entity's members or participants. This can be achieved by posting the required information on a website accessible to all members or participants.¹² For non-major SCI events, the required information must be disseminated only to the members or participants that may be affected by the event.

Information disseminated to an SCI entity's members or participants must be accurate and should provide sufficient detail to permit members or participants to determine the nature and scope of any effect from an SCI event. The requirement that information be provided "promptly" allows an SCI entity limited discretion in to determine the most efficient manner of dissemination and to allow accurate information to be collected by the entity.

The Commission noted that the occurrence of a systems compliance issue at an SCI entity does not necessarily mean that an SCI entity has violated Regulation SCI. The rule requires the systems compliance policies and procedures be reasonably designed; the Commission acknowledged that reasonable policies and procedures will not ensure elimination of all systems issues. However, a systems compliance issue may be probative of reasonableness. The Commission plans to exercise its discretion to initiate an enforcement action. Similarly, reporting SCI events to the Commission does not necessarily mean the SCI entity has violated Regulation SCI, or the Exchange Act as a whole.

Liability under Regulation SCI is separate from liability for other violations that arise from an underlying event; compliance with Regulation SCI is not a safe harbor from liability under other laws or rules.

Rule 1003 – Testing and Reporting for SCI Systems

Rule 1003 addresses the reporting responsibility of SCI entities and the mandated systems testing they must perform.

Reports on Changes. Under Rule 1003(a), all SCI entities must provide the Commission with a report describing the past, present and future material changes to any SCI system or indirect SCI system. These

reports must include the dates of commencement and completion (or proposed dates), as well as the nature of the changes to the system. The reports must be submitted on a quarterly basis and must cover the prior, current and subsequent calendar quarters. Though these reports must be submitted for all changes intended to occur in the subsequent quarter, the Commission emphasizes that this reporting is meant strictly for oversight purposes and will not evolve into a pre-approval process.

There is no prescribed form or method for such reporting, instead each SCI entity may determine how to report material changes. Furthermore, SCI entities are given discretion to decide what materiality means in the context of their business. Regulation SCI simply mandates that each firm establish reasonable written criteria for identifying such a change to an SCI system or indirect SCI system and report changes that meet that threshold.

Rule 1003(a) also imposes a supplemental reporting requirement to correct any material errors or material omissions in a previously submitted quarterly report.

Reviews and Testing of SCI Systems. Rule 1003(b) requires all SCI entities to conduct a review of all SCI systems and indirect SCI systems on a regular basis. These tests must meet two distinct requirements. First, SCI entities must run a risk assessment of all SCI systems and indirect SCI systems. Second, SCI entities must conduct an assessment of the internal control design and effectiveness. This includes an examination of the physical and logical separation of non-SCI systems, development processes and information technology governance of the SCI entity, and should be guided by industry standards.

Each SCI entity is given the discretion to design and implement their own testing methods and standards, so long as they achieve the regulatory objectives outlined above. The review process must be carried out by appropriate personnel and with appropriate regularity. The person conducting the review, whether an employee or third-party, must be qualified to do so and must be sufficiently disinterested in the outcome to be considered objective in his or her testing. These reviews must occur at least once every twelve months with the exception of market regulation systems, market surveillance systems and penetration testing of the SCI entity's network, all of which must be reviewed once every three years.

Each review must be recorded and submitted to senior management at the SCI entity within 30 days of the review's completion. In addition, the report must be submitted to the SCI entity's Board of Directors and the Commission no more than 60 days after senior management¹³ receives it.

Rule 1004 – Business Continuity and Disaster Recovery Plans

Rule 1004 addresses business continuity and disaster recovery plans (BC/DR) of SCI entities. All SCI entities must develop and adopt standards to designate which of its members and participants are taken as a whole, the minimum necessary for the maintenance of fair and orderly markets if a BC/DR plan must be activated. SCI entities must then identify the members meeting that criteria and require their participation in annual BC/DR testing.

SCI entities are afforded flexibility in determining the exact nature and process of testing. Still, the Commission mandates that these reviews include both general functional and performance testing as well as a specific reviews of the SCI entity's systems dealing with order entry and execution, clearance and settlement, order routing and the transmission or receipt of market data. However, these reviews need not consist of a stress test, and the SCI Regulation does not expect that the BC/DR facilities replicate the speed, capacity or other features of the primary site.

BC/DR testing under Rule 1004 must be conducted as an industry- or sector-wide exercise. SCI Entities must coordinate with each other in order to develop the script, method and timing of such testing, as the

Commission will not serve as an intermediary. Given the complexities inherent in such large-scale coordination, this element of Regulation SCI will not be enforced until 21 months from the effective date.

Rule 1004 requires recordkeeping and record retention, but there is no reporting obligation. Rather than filing with the Commission after each BC/DR review, the SCI entity must only keep their report on file and available for review.

Rule 1005 and Rule 1007 – Recordkeeping

Rule 1005 of Regulation SCI sets forth the recordkeeping requirements for an SCI entity. If the entity is an SCI SRO, such entity must apply the existing requirements of Rule 17a-1 to Regulation SCI compliance-related documents. If the SCI entity is not an SCI SRO, Regulation SCI still imposes similar requirements. Such an entity must:

- Make, keep and preserve 1 copy of all documents relating to compliance with Regulation SCI, including changes to SCI systems and indirect SCI systems
- Keep all such documents for not less than five years, the first two in a place that is readily accessible to the Commission for inspection and examination
- Upon request, promptly furnish copies of any such documents to the Commission

Documents includes all correspondence, memoranda, papers, books, notices, account, and other such records made and received in the course of business related to Regulation SCI compliance. Upon ceasing business or ceasing to be registered with the Commission, an SCI entity must take all necessary action to ensure the above mentioned documentation is maintained and accessible for the same required duration.

Third Parties. An SCI entity retains legal responsibility for systems operated on its behalf. SCI entities are therefore responsible for ensuring that necessary documents are produced, retained and made available by the third party, as if the records were kept by the SCI entity itself. The SCI entity should have a system in place to ensure it is able to meet these recordkeeping requirements.

Similarly, Rule 1007 states that if any records or files which Regulation SCI requires an SCI entity to keep are prepared or maintained by a service bureau on behalf of the SCI entity, the SCI entity must ensure records are available to the Commission by submitting a written undertaking by such service bureau, signed by a duly authorized person at such service bureau. The written undertaking must include an agreement by the service bureau to permit the Commission to examine such records and promptly furnish to the Commission true, correct and current electronic files or hard copies of such records upon request, under the same retention period required of the SCI entity itself. Use of such a service bureau does not relieve an SCI entity of its responsibility to prepare and maintain such records and provide access to the Commission.¹⁴

Rule 1006 – Electronic Filing and Submission

Any Regulation SCI-required submissions to the Commission should be filed using Form SCI — except for the immediate notification and periodic updates provided to the Commission pursuant to Rule 1002(b). Form SCI should be filed through the Electronic Form Filing System (EFFS) in a text-searchable format. Form SCI must be submitted with an electronic signature, and an SCI entity must also retain a manually signed copy of the signature page. Form SCI and instructions can be found at page 724 of the Regulation SCI release.¹⁵

To allow the electronic filing of Form SCI, the Commission has adopted an amendment to Rule 24b-2. The amendment provides an electronic means of requesting confidential treatment of filings on Form SCI, an exception from the paper-only requirement of Rule 24b-2.

Effective Dates and Compliance Dates

Regulation SCI will become effective **February 3, 2015** (Effective Date). The Compliance Date is 9 months after the Effective Date — **November 3, 2015**. Exceptions include: (i) ATs newly meeting volume thresholds in definition of SCI ATS, which will have an additional six months from the time they reach the threshold; and (ii) the industry- or sector-wide coordinated testing requirement, which kicks in 21 months from the Effective Date — **November 3, 2016** — for SCI entities to coordinate testing of BC/DR plans on an industry or sector-wide basis with other SCI entities.

Conclusion

Given the detailed nature of Regulation SCI, covered entities should take steps now to ensure they are in compliance, well before the November 2015 effective date. While the regulation currently covers a limited constellation of businesses, the SEC's own statement indicates a possibly wider remit in the future.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

[Vivian Maese](#)
vivian.maese@lw.com
+1.212.906.1302
New York

[Stephen P. Wink](#)
stephen.wink@lw.com
+1.212.906.1229
New York

The author would like to thank for Tiana Hertel, Adrian Ramos and Matthew Wynne their contributions to this *Client Alert*.

You Might Also Be Interested In

[Virtual Currencies: New York State Department of Financial Services Discusses Proposed Regulations](#)

[GMAC/CFTC Hosts Open Meeting Regarding Bitcoin and Digital Currency](#)

[Virtual Currencies: New York State Department of Financial Services Releases Proposed Regulations](#)

Client Alert is published by Latham & Watkins as a news reporting service to clients and other friends. The information contained in this publication should not be construed as legal advice. Should further analysis or explanation of the subject matter be required, please contact the lawyer with whom you normally consult. The invitation to contact is not a solicitation for legal work under the laws of any jurisdiction in which Latham lawyers are not authorized to practice. A complete list of Latham's *Client Alerts* can be found at www.lw.com. If you wish to update your contact details or customize the

information you receive from Latham & Watkins, visit <http://events.lw.com/reaction/subscriptionpage.html> to subscribe to the firm's global client mailings program.

Endnotes

- ¹ See Chair Mary Jo White, Statement at Open Meeting on Regulation SCI (Nov. 19, 2014).
- ² Fixed income ATSS are still subject to Rule 301(b)(6) of Regulation ATS.
- ³ FINRA members already subject to similar requirements under FINRA Rule 4370 should note that Regulation SCI goes further in its detailed timing, testing and coordination requirements.
- ⁴ Authoritative bodies include: a US governmental entity or agency, an association of US governmental entities or agencies or a widely recognized organization
- ⁵ <http://www.sec.gov/rules/final/2014/staff-guidance-current-sci-industry-standards.pdf>
- ⁶ The reporting obligations in Regulation SCI do not affect obligations under other securities laws (e.g. Regulation S-K and Regulation FD).
- ⁷ Entities can request confidential treatment under Rule 24b-2, but does that mean that all other notifications/communications are available to public. Also the commentary specifically said: "while information submitted to the Commission pursuant to Regulation SCI will generally be treated as confidential and subject to Rule 24b-2, it may be subject to FOIA requests."
- ⁸ This should include a description of the root cause of the SCI event.
- ⁹ This is meant to assess compliance with the disclosure requirements of Rule 1002.
- ¹⁰ If an event affects other systems in addition to market regulation or surveillance systems, an SCI entity must still disseminate information on other systems.
- ¹¹ A "major SCI event" means an SCI event that has, had or the SCI entity reasonably estimates would have: (a) any impact on a critical SCI system; or (b) a significant impact on the SCI entity's operations or on market participants.
- ¹² Rule 1002 does not require public dissemination.
- ¹³ For the purposes of Rule 1003(b), "senior management" is defined as the CEO, CTO, CIO, GC and/or the CCO of an SCI entity.
- ¹⁴ These requirements are substantially the same as the requirement applicable to broker-dealers under Rule 17a-4(i) of the Exchange Act.
- ¹⁵ See Release No. 34-73639, <http://www.sec.gov/rules/final/2014/34-73639.pdf> (Nov. 19, 2014).